PROCEDURE FOR THE PROTECTION OF COMPUTER SOFTWARE AND/OR COMPUTER-READABLE DATA AS WELL AS PROTECTIVE EQUIPMENT

BACKGROUND

[0001] The invention involves a procedure to protect computer software and/or computer-readable data against unauthorized use as well as a protective device for use in such a procedure.

[0002] Computer software, documents, and data with content that are to be protected against illegal dissemination are primarily sold individually as a package. In part technical measures are employed against unauthorized use, including in particular pirate copies, whereby the measures are either pure software solutions or a hardware protection, so-called dongle.

[0003] Problematic in any kind of security measures against unauthorized use is that individually adjusted security measures are required for every product. New distribution paths such as ESD (electronic software distribution), for example over the Internet, are made much more difficult because along with the protected computer program or protected data it is always necessary to prepare and provide individual hardware and software. The licenser therefore has additional costs just for the security measures. The licensee has a one-time procurement price and risks making a bad investment. Payment according to the intensity of use is not customary, because it cannot be measured technically.

[0004] The high-grade procedures available today to protect software on the basis of the encoding of documents, program code, or resources are not adequate for future security requirements, especially for widespread and accordingly reasonably priced software as well as their secure accounting as a function of use.

[0005] The currently available Private Key Tokens that are used for authentication and that can store certificates, for example in accordance with ITU-norm X.509v3, do meet high security requirements but permit only the storage of a few certificates. The simultaneous use of many differently protected programs or data with individual encoding and accounting is also not foreseen here.

[0006] Because every individual software product requires its own protective procedure that in any case is associated with substantial additional costs, the overwhelming share of computer software and/or computer-readable data is still disseminated without effective copy protection. The originators or licensers thereby miss receiving large sums of unpaid license fees.

[0007] For the future use of many different computer programs or computer-readable data, especially also from different licensers and utilizing new online marketing paths, new protective procedures are therefore needed that secure the income of licensers and correspond to increased security requirements.

[0008] US 5 826 011 describes an electronic security device developed as hardware for the protection of computer software in the installation, which is linked to the computer of the user. This electronic security device includes different secret installation data that are required in the installation of the protected program.

[0009] US 5 805 802 describes a module for the protection of software in a computer network, including a microprocessor for the implementation of controlled access to the software, an interface for linking with a network server, a programmable memory in which a use-restricting code is stored, and a device for the processing of this use-restricting code and a current user number.

[0010] WO 00/20948 describes a copy protection system that combines a signature procedure with a coding or encoding procedure using variable keys.

[0011] Finally the company publication "WIBU-KEY - the Convincing Concept on the Theme of Copy protection" from the applicant himself, published in 1999 by WIBU-SYSTEMS AG, describes a protective device developed as a hardware supplement for linking a copy-protected software to the computer of the licensee. Here use is made of a procedure in which the software to be protected is encoded at the licenser and again decoded at the licensee. The encoding depends upon three parameters: the Firm Code that is given by producer and issued just once for each licenser; the User Code that the

licenser is free to set; and finally the Selection Code that serves to select one of more than 4 billion encoding variants for each license entry. The Firm Code and the User Code are programmed into the protective device by the licenser. The Selection Code is sent to the protective device at the disposal of the licensee in the initializing of the encoding and is not stored. The Selection Code, prepared by the licenser, is included in the protected data or the protected software.

[0012] Detrimental in the last-named protective procedure is the fact that the licenser is dependent on a fixed Firm Code provided by the producer of the procedure or of the protective device (box). This results in a certain dependency of the licenser upon the producer of the procedure or of the box, which on the one hand restricts the licenser whereas from the point of view of the licenser it leads to security that is not yet optimal. Furthermore, a substantial advantage is that every licenser requires a certain fixed Firm Code, which for the licensee, that is, the end customer of the software, may mean that in using the software of different licensers he must employ several protective devices.

SUMMARY OF THE INVENTION

[0013] Hence the invention is based on the technical problem of making available an improved system for the protection of computer software and/or computer-readable data against unauthorized use that makes possible simultaneous use by many licensers for many products at a time independently of each other.

[0014] The solution of this problem is based on a procedure in which the software or the data of the licenser is protected through individual encoding depending on license parameters.

[0015] The problem is also solved in that the encoding of the software or data is initialized at the licenser dependent on a secret Firm Key freely choosable by the licenser, that the encoding of the transmission of the license parameters from the licenser to the licensee takes place dependent on a secret Private Serial Key, and that the decoding of the

protected software or data is initialized at the licensee dependent on the Firm Key selected by the licenser.

[0016] The advantage of the procedure in accordance with the invention is in the fact in particular that many mutually independent license parameters coming from different licensers for in each case different software or data can be utilized, whereby the use of the Private Serial Key ensures that the installation, modification, and deletion of license parameters can take place only at the one licensee and not at other licensees, because they do not have the identical Private Serial Key SK. For this reason, a manipulation of the license parameters is not possible, because these cannot be decoded. This makes it possible to carry out the license parameters in insecure transmission paths such as the Internet, for example, without this causing a loss of security for the licenser.

[0017] An additional great advantage of the procedure in accordance with the invention is that the licensee of a copy-protected software, that is, the end customer, must employ just a single procedure even if he wants to use a multitude of different software items from several different licensers. This not only substantially reduces the costs of the copy protection for both the licenser and the licensee but also raises in particular the acceptance at the licensee.

[0018] The security of the procedure for the licenser is further increased when the secret Private Serial Key is produced randomly at the licensee, indeed without the licenser, the licensee, or anyone else being able to influence that.

[0019] Preferably the licensee is firmly assigned a unique serial number and the signature of the transmission of the license parameters from the licenser to the licensee occurs dependent on this serial number.

[0020] In an advantageous development of the procedure in accordance with the invention, each licenser is assigned a secret Firm Common Key by the producer of the procedure. Through an encoding dependent on the Firm Code of the respective licenser, this is calculated from a secret Common Key, which is also not revealed to the licenser. Each licenser receives only the Firm Common Key that fits his Firm Code. The

Firm Common Key is needed to verify the installation, changing, or deletion of license parameters.

[0021] Preferably the storage of the license parameters occurs inside a protective device (box) developed as a hardware supplement, which is linked to an interface of the computer of the licensee. This protective device contains the decoder necessary for the automatic decoding of the protected software or data.

[0022] Not only to secure computer software or computer-readable data against unauthorized use but also to bill for its use dependent on the intensity of the use, a limiter can be provided for the licensee that limits the time period and/or the number of decodings of the protected software or data. In this connection, a date and/or time information can be transmitted from a reference source to the licensee in an optimum way secure from manipulation. Preferably this limiter is likewise a component of the protective device.

[0023] In a further advantageous configuration of the procedure in accordance with the invention, a secret Private Box Key determined by the producer, who makes available a Public Box Key, is stored in the protective device. The producer likewise makes available a list of valid Public Box Keys. The Private Box Key is not dependent on the licensee and licenser and can therefore be used for software or data of different licensers. The Public Box Key calculated from the Private Box Key is used for the encoding of the transmission of license parameters between the licenser and licensee. By checking the validity of the Public Box Keys, one prevents an attacker from delivering any Public Box Key that he has ascertained from an invalid Private Box Key selected by him and thereby decoding the data transmitted by the licenser.

[0024] A protective device in accordance with the invention includes an arrangement that contains a random secret Private Serial Key for the encoding of the transmission of the license parameters between the licenser and licensee. If the memory in the protective device includes several memory areas for the storage of license parameters of different licensers, then the same protective device can be used by the licensee in

connection with software or data of a multitude of different licensers.

[0025] A particularly large degree of security for the licenser can be achieved in that the microprocessor, the memory for the license parameters, the decoder, and the installation for the production of the Private Serial Key are developed on a single integrated semiconductor circuit, especially an ASIC (Application Specific Integrated Circuit). In this way, one prevents in particular the possibility of direct manipulation of the memory with the stored license parameters.

[0026] A use-dependent accounting with the licenser is possible if the protective device also includes a limiter secure against manipulation that limits the time period and/or the number of decodings of the protected software or data.

[0027] An embodiment example of the invention is explained in more detail below through the enclosed figures and lists.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

[0028] Figure 1 is a diagram showing a procedure for the protection of computer software and/or computer-readable data including accounting for their use by employing a protective device developed as a hardware supplement;

[0029] Figure 2a is a diagram showing the keys and data at the producer of the procedure and protective device in accordance with Figure 1;

[0030] Figure 2b is a diagram showing the keys and data at the licenser;

[0031] Figure 3 is a diagram showing the keys and data at the licensee;

[0032] Figure 4 is a flow chart of the installation of a license parameter by a new licenser;

[0033] Figure 5 is a flow chart of the deletion of a license parameter;

[0034] Figure 6 is a flow chart of the installation, modification, or deletion of a license parameter;

[0035] Figure 7 is a flow chart of the initialization of a decoding at the licensee; and

[0036] Figure 8 is a flow chart of the setting of an expiration date.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0037] The procedure schematically presented in Figure 1 makes possible both the protection and the use-dependent accounting of computer software and/or computer-readable data of a multitude of licensers 1, 2, to n. The software or data is/are first stored on servers of the licenser and can be downloaded through the Internet to the computer of a licensee.

[0038] On the computer of the licensee is a protective device (box) 3 developed as a hardware supplement that is linked through an interface 4 to the computer 2 of the licensee.

[0039] The protective device 3 includes a microprocessor 5, and a nonvolatile memory (EEPROM) with several memory areas 6a, 6b, 6c, the number of which corresponds to the number of the licenser 1, 2, to n.

[0040] The protective device 3 also includes an encoder and decoder 7 as well as an installation 8 for the production of a random secret Private Serial Key SK. A limiter 9 is also foreseen to limit the time period and/or the number of the decoding of the protected software or data.

[0041] All essential parts of the protective device 3, hence in particular the microprocessor 5, the memory 6, the encoder and decoder 7, and the installation 8 for the production of the Private Serial Key SK, are developed on a single integrated semiconductor, a so-called ASIC (Application Specific Integrated Circuit), which is surrounded by a stable housing 10 made of plastic, for example.

[0042] The following will describe which keys and data are produced and stored at the producer, the licenser, or the licensee and whether these are secret or public.

[0043] The list of Figure 2a includes the keys and data at the producer of the procedure and the protective device. This includes a secret Common Key (CK), which is used for the production of a secret Firm Common Key (FCK) for a particular licenser. The producer also selects a Private Box Key (BK), which is secret and makes available a Public Box Key derived

from it. The Private Box Key (BK) is independent of the licensee and can be identical for the use of the procedure with every licenser. The Public Box Key is used for the encoding of the sequence for the installation or deletion of license parameters that are transmitted from a licenser to a licensee. Not absolutely necessary is a secret Private Validation Key (VK) selected by the producer. The associated Public Validation Key is stored at the producer. The licenser can decide whether or not the functionality should be used with the Validation Key (VK). The Validation Key (VK) is used to transmit reference information such as, for example, the current date and time from a reference source, e.g., a trust center, to the licensee securely encoded against manipulation.

[0044] In accordance with the list of Figure 2b, a licenser has the public Firm Code (FC) that the producer makes available to him. The producer makes the secret Firm Common Key (FCK) available to the licenser for his Firm Code (FC). The licenser can freely set his own secret Firm Key (FK) independently of the producer. The Firm Key (FK) is used as a secret key for the installation and modification of license parameters of the licenser and as a secret key for the creation of an encoding sequence. The licenser also has a Public Box Key (BKp) made available by the producer.

[0045] The list of Figure 3 includes the keys and data that are contained in the protective device (3, see Figure 1) at the licensee. This initially includes a secret unique Private Validation Key (VK) that was selected by the producer of the protective equipment 3.

[0046] Optionally date and time information (Time Date Stamp, TDS) can be transmitted secure from manipulation from a reference source to the licensee. The Validation Key (VK) is needed for this. Also at the licensee is the secret Private Box Key (BK), whose Public Box Key (BKp) was made available publicly by the producer of the protective device.

[0047] Especially important for security is the Private Serial Key (SK) randomly produced at the licensee, which is completely independent both of the producer and of a licenser. This Private Serial Key (SK) makes available a Public Serial

Key (SKp), which is used for the encoding of the data transmission between the licenser and licensee.

[0048] The licensee also has the unique Serial Number (SN) as well as the secret Common Key (CK) from which the Firm Common Key (FCK) is calculated through an encoding dependent on the Firm Code (FC).

[0049] The memory 6 of the protective device 3 at the licensee (see Figure 1) includes in the three memory areas 6a, 6b, and 6c shown here as an example the license parameters needed for the use of the protected software or data. These license parameters consist of a Firm Item (FI) for each licenser and one or more User Items, which in each case are assigned to a Firm Item.

[0050] Firm Items 1, 2, and 3 consist in each case of the Firm Code (FC) of the respective licenser, a Firm Programming Counter (FPC), the secret Firm Key (FK) of the concerned licenser, and a public temporary Session ID (SID).

[0051] The several User Items which are each assigned to a Firm Item include in each case a User Code (UC), a Master Mask (MM) for the variable availability for different program modules, functions, etc., User Data (UD), an expiration date (ED), a Limit Counter (LC), and a Network Use Counter (NUC).

[0052] Described below are the steps relevant to security in the application of the procedure and the transmission of the keys and data between the licenser and licensee in a public transmission path such as the Internet.

[0053] For the use of the protected software or data, the licensee needs valid license parameters that include a Firm Item and a User Item. The flow chart in Figure 4 explains the installation of a new Firm Item at the licensee.

[0054] Initially a temporary Firm Item is installed and a random Session ID (SID) is produced in the protective device of the licensee. This Session ID (SID), the concerned Public Box Key (BKp), and the Public Serial Key (SKp) derived from the Serial Key (SK) are then sent through the Internet to the licenser to obtain a Firm Creation Sequence. The use of the random Session ID (SID) prevents the possibility of the later repetition of an operation carried out to install a license parameter at the same licensee.

[0055] The licenser now checks whether the Public Box Key (BKp) received from the licensee is permissible. The comparison occurs with a list of the valid Public Box Keys (BKp) that the licenser has obtained from the producer of the protective device. Without this authentication, an attacker could transmit to the licenser any Public Keys for which he has the Private Keys and then learn the licenser's secret Firm Key (FK) included in the Firm Item Creation Sequence.

[0056] The licenser now calculates a sequence that is composed of the Firm Code (FC), Firm Common Key (FCK), the Firm Key (FK) selected by him, and the previously obtained Session ID (SID). In the first step, this sequence is encoded with the Public Serial Key (SKp), which previously was transmitted by the licensee. This ensures that the sequence can be decoded only by this licensee, because no one else has the associated Private Serial Key (SK).

[0057] In the next step, the so encoded sequence is encoded with the Public Box Key (BKp). Only the licensee has the Private Box Key (BK) to decode the sequence again. This ensures that no unauthorized person can decode the sequence, because he does not know the Private Box Key (BK) necessary for the decoding. The so-encoded Firm Item Creation Sequence is then transmitted to the licensee over the Internet.

[0058] In the protective device of the licensee, the received Firm Item Creation Sequence is decoded with the Private Box Key (BK). The Private Box Key (BK) is secret and known only to the producer of the protective device. It is therefore ensured that no potential attacker can decode the Firm Item Creation Sequence that contains the Firm Key (FK) of the licenser.

[0059] The previously only half-decoded Firm Item Creation Sequence is completely decoded with the Private Serial Key (SK). The Private Serial Key (SK) was randomly produced in the protective device of the licensee and hence is not accessible to anyone. For this reason, the decoding of the sequence is extremely effectively protected. Other licensees or their protective devices cannot decode the sequence; this is not even possible for the producer of the protective device.

[0060] It is then checked whether a temporary Firm Item was installed with the Session ID (SID) contained in the Firm Item Creation Sequence and whether the Firm Code (FC) fits the Firm Common Key (FCK). If not, the Firm Item is not installed. If so, the temporary Firm Item now becomes a permanent and usable Firm Item. The Firm Code (FC) and the secret Firm Key (FK) are stored in the protective device of the licenser. At the same time, a Firm Programming Counter is set at zero.

[0061] The flow chart of Figure 5 shows how a Firm Item from the memory of the protective device of the licensee is deleted. The deletion of a Firm Item is not relevant to security. For the licensee, however, it is important that the deletion of a Firm Item cannot occur unintentionally or through an unauthorized person.

[0062] To complete the license parameters belonging to a certain software, a User Item must be added to a Firm Item. In installation this User Item contains at least the User Code (UC). Optionally the User Item can contain a Master Mask (MM), a limiting counter, an expiration date, a Network Use Counter (NUC), or other added data. The changing of a User Item occurs through the modification of existing parts or the adding of new elements.

[0063] Figure 6 explains the fundamental steps for the installation, modification, or deletion of a User Item by means of a User Item Change Sequence (UICS).

[0064] So that the licensee can make use of authorization granted him by the licenser and utilize a protected computer software and/or protected computer-readable data, a decoding must be initialized at the licensee. The process is shown in Figure 7.

[0065] The following keys or data are needed to produce a decoding sequence: Firm Code (FC), User Code (UC), Firm Key (FK), and a Selection Code supplied as a parameter of the protected software.

[0066] Depending on the chosen Selection Code, the expiration date is checked and/or the limiting counter is reduced by a certain value. The decoding can be initialized and correctly carried out only if valid license parameters are present that contain the corresponding Firm Code (FC) and User

Code (UC) and their limiting counter or expiration date has not run out.

[0067] The flow chart in Figure 8 explains the setting of a validated time/date information (Time Date Stamp, TDS). This information cannot be manipulated. The limiter (9) uses this information to limit the time period of use of the protected software or data by the licensee.

[0068] To set a valid reference time to check the expiration dates, a reference time by date and clock time, which is encoded with the Public Validation Key (VKp) at the licensee, is set by an authorized secure position that has the Serial Number (SN) and the Public Validation Key (VKp). Only the licensee has the Private Validation Key (VK) and can decode this time reference. This ensures that the reference time cannot be changed by an unauthorized person. In addition, the authorized position can block the complete process at the licensee if this is employed as an option by the licenser, for example in the event of abuse by the licensee.

[0069] Compilation of the Reference Symbols for Figure 1

1	1a, 1b, 1c server of the licenser
2	Computer of the licensee
3	Protective device
4	Interface
5	Microcomputer
6	Memory
6a,6b,6c	Memory means (of 6)
7	Encoder/decoder
8	Installation for the production of SK
9	Limiter
10	Housing